

# A construction of group divisible designs with zero block sum

Chong-Dao Lee\*      Yaotsu Chang<sup>†</sup>      Chia-an Liu<sup>‡</sup> §

December 30, 2016

## Abstract

This paper gives a construction of group divisible designs on the binary extension fields with block sizes 3, 4, 5, 6, and 7, respectively, which is motivated from the decoding of binary quadratic residue codes. A conjecture is proposed for this construction of group divisible designs with larger block sizes.

**Keywords:** Group divisible design (GDD), finite field, quadratic residue code.

**2010 MSC:** 05B05, 51E05.

## 1 Introduction

Assmus and Mattson in 1969 [2] first proposed balanced incomplete block designs (BIBDs) via the theory of error-correcting codes. The codewords of any fixed weight in an extended quadratic residue code [2] (respectively, a Reed-Muller code [6], an extremal binary doubly-even self-dual code [6], and a Pless symmetry code [15]) form a 2-design (respectively, 3-design, 5-design,

---

\*Department of Communication Engineering, I-Shou University, Kaohsiung, Taiwan

<sup>†</sup>Department of Financial and Computational Mathematics, I-Shou University, Kaohsiung, Taiwan

<sup>‡</sup>Corresponding author. E-mail address: liuchiaan8@gmail.com (C.-a. Liu).

§Department of Financial and Computational Mathematics, I-Shou University, Kaohsiung, Taiwan

and 5-design). The minimum weight codewords in a linear perfect code [3] with minimum distance  $d = 2e + 1$  support an  $(e + 1)$ -design. It was shown in [14] that the codewords of any fixed weight in two codes, an extremal binary even formally self-dual code and its dual code, forms a 3-design. For more  $t$ -designs supported by other error-correcting codes, the reader is referred to [5]. From the above results, the codewords of error-correcting codes play a significant role in constructing BIBDs. In the theoretical aspect, the study on  $t$ -designs over finite fields [4, 11] also gets some attention.

The group divisible design (GDD) is a topic generalized from the pairwise balanced design (well-known as PBD) [1, Definition 1.4.1]. Since GDD has been widely applied to graphs [12] and matrices [18], many authors proposed different constructions of a GDD. One can see [12, 18, 13], [1, Definition 1.4.2], [19, Definition 7.14] and [21, Definition 5.5] for some examples. Recently, GDDs have been used in the constructions of optical orthogonal codes [24] [23], constant-weight codes [9] [7], and constant-composition codes [8]. However, there are very few studies focused on GDDs constructed from error-correcting codes.

In 2003, Chang *et al.* [10] developed the new decoders for three binary quadratic residue codes with irreducible polynomials. Motivated by the decoding of binary quadratic residue codes, this study considers the problem of constructing GDD. A *group divisible design*  $\text{GDD}(v, n, k)$  is a triple  $(X, \mathcal{G}, \mathcal{B})$ , where  $\mathcal{G}$  is a collection of  $n$ -subsets of  $v$ -set  $X$  and  $\mathcal{B}$  is a collection of  $k$ -subsets of  $X$ . In this paper, we assume  $X = \mathbb{F}_{2^m} \setminus \{0, 1\}$  and consider the correctable error patterns  $(x_1, x_2, \dots, x_k)$  with a fixed weight  $k$  and satisfying  $\alpha^{x_1} + \alpha^{x_2} + \dots + \alpha^{x_k} = 1$  in the finite field  $\mathbb{F}_{2^m}$ , where distinct integers  $1 \leq x_i \leq 2^m - 1$  for  $1 \leq i \leq k \leq m$  and  $\alpha$  is a primitive element of  $\mathbb{F}_{2^m}$ . If  $k = 2$ , then those error patterns form a group set  $\mathcal{G}$ . Similarly, for each  $3 \leq k \leq m$ , these error patterns support a block set  $\mathcal{B}$ . This paper gives a construction of group divisible designs with block sizes 3, 4, 5, 6, and 7, respectively. The correctness and parameters of the construction are obtained by using the inclusion-exclusion principle.

The paper is organized as follows. Preliminary notations are introduced in Section 2. The details of our construction of GDDs are proposed in Section 3. Section 4 summarizes the results obtained from Section 3 and presents a conjecture for group divisible designs with larger block sizes.

## 2 Preliminary

Basic results of the group divisible design and finite field are provided in this section for later used. The notations and definitions of a GDD can be referred to [1, Definition 1.4.2].

**Definition 2.1.** A *group divisible design*  $\text{GDD}(v, n, k)$  is a triple  $(X, \mathcal{G}, \mathcal{B})$ , where  $\mathcal{G}$  is a collection of  $n$ -subsets of  $v$ -set  $X$  and  $\mathcal{B}$  is a collection of  $k$ -subsets of  $X$ . We say that  $\mathcal{G}$  is the *group set* and each element in  $\mathcal{G}$  is a *group*, and  $\mathcal{B}$  is the *block set* and each element in  $\mathcal{B}$  is a *block*, such that:

- (i)  $\mathcal{G}$  forms a partition of  $X$ ,
- (ii) for all  $B \in \mathcal{B}$  and  $u, v \in B$  there does not exist  $G \in \mathcal{G}$  such that  $u, v \in G$ , and
- (iii) every pair of distinct elements  $x$  and  $y$  from different groups occur together in exactly  $\lambda$  blocks.

In particular, the condition (iii) is called the *balance condition*, and  $\lambda$  is called the *balance parameter* of  $(X, \mathcal{G}, \mathcal{B})$ .

Let  $(X, \mathcal{G}, \mathcal{B})$  be a GDD and  $r_x$  denote the number of blocks in  $\mathcal{B}$  that contain  $x$  for each  $x \in X$ . The following result given in [20, Proposition 2.2] tells that  $r_x$  is independent of the choice of  $x$  which is called the *repetition number* of  $(X, \mathcal{G}, \mathcal{B})$ .

**Proposition 2.2.** *Let  $(X, \mathcal{G}, \mathcal{B})$  be a  $\text{GDD}(v, n, k)$  with balance parameter  $\lambda$ . Then each element in  $X$  occurs in*

$$r = \frac{\lambda(v - n)}{k - 1} \tag{2.1}$$

*blocks.*

Let  $r = r_x$  be the repetition number of  $(X, \mathcal{G}, \mathcal{B})$ . Since each block in  $\mathcal{B}$  is of cardinality  $k$ , one can get the number of blocks in  $\mathcal{B}$ , denoted by  $b = |\mathcal{B}|$ , by direct counting method.

**Proposition 2.3.** *Let  $(X, \mathcal{G}, \mathcal{B})$  be a  $GDD(v, n, k)$  with balance parameter  $\lambda$  and repetition number  $r$ . Then, the number of blocks in  $\mathcal{B}$  is*

$$b = |\mathcal{B}| = \frac{vr}{k}. \quad (2.2)$$

□

The finite field properties in the following are referred to [16, Sec 4.2].

- (i) Every finite field has  $p^m$  elements for some prime  $p$  and positive integer  $m$ .
- (ii) For any positive integer  $m$ , there is a unique field (up to isomorphism) of  $2^m$  elements. We denote this field by  $\mathbb{F}_{2^m}$ .
- (iii) The multiplicative group  $\mathbb{F}_{2^m} \setminus \{0\}$  is cyclic so that there exists a generator (which is so-called a *primitive element*) of  $\mathbb{F}_{2^m} \setminus \{0\}$ .

Finite field is an important topic in Abstract Algebra. See [22, Chapter 6] for more details.

Throughout this paper, one considers  $X = \mathbb{F}_{2^m} \setminus \{0, 1\}$ , where 0 and 1, respectively, denote the zero and unity elements in the finite field  $\mathbb{F}_{2^m}$  of order  $2^m$  for arbitrary positive integer  $m \geq 3$ . Note that the cardinality of  $X$  is  $|X| = 2^m - 2$ .

### 3 A construction of group divisible designs

The aim of this section is to propose a construction of group divisible designs with block sizes 3, 4, 5, 6, and 7. The collections  $W_k$  of  $k$ -subsets of  $X$  for  $k \geq 2$  are given in the following. It will be verified that  $W_2$  forms a partition of  $X$ , and for each  $3 \leq k \leq 7$  a GDD with block size  $k$  is constructed from  $W_k$ .

**Definition 3.1.** For each positive integers  $k \geq 2$ , let

$$W_k = \{B \subset X \mid |B| = k, \sum_{i \in B} i = 1, \text{ and } \binom{B}{\ell} \cap W_\ell = \emptyset \text{ for all } 2 \leq \ell \leq k-3\}.$$

The next observations are directly from Definition 3.1.

**Remark 3.2.** The condition  $\binom{B}{\ell} \cap W_\ell = \phi$  for all  $2 \leq \ell \leq k-3$  in Definition 3.1 can be realized as for all  $2 \leq \ell \leq k-1$ . From the condition  $|B| = k$ , if  $x \in \binom{B}{k-1} \cap W_{k-1}$ , then the only element in  $B \setminus \{x\}$  is 0. However,  $0 \notin B \subset X$ , which is a contradiction. If  $y \in \binom{B}{k-2} \cap W_{k-2}$ , then the sum of  $B \setminus \{x\}$  is 0 so that the two elements in  $B \setminus \{x\}$  are equal, which also contradicts to  $|B| = k$ .

An example of  $W_2$  and  $W_3$  is illustrated.

**Example 3.3.** Let  $m = 3$ . Let  $\gamma = x$  be a primitive element of the finite field  $\mathbb{F}_{2^3} \cong \mathbb{F}_2[x]/\langle x^3 + x + 1 \rangle$ . Then, one has  $\gamma^2 = x^2$ ,  $\gamma^3 = x + 1$ ,  $\gamma^4 = x^2 + x$ ,  $\gamma^5 = x^2 + x + 1$ , and  $\gamma^6 = x^2 + 1$ . Let  $X = \{\gamma^i \mid i = 1, 2, \dots, 6\}$ . From Definition 3.1, the collection  $W_2$  of 2-subsets of  $X$  is

$$W_2 = \{\{\gamma, \gamma^3\}, \{\gamma^2, \gamma^6\}, \{\gamma^4, \gamma^5\}\}$$

which forms a partition of  $X$ , and the collection  $W_3$  of 3-subsets of  $X$  is

$$W_3 = \{\{\gamma, \gamma^2, \gamma^5\}, \{\gamma, \gamma^6, \gamma^4\}, \{\gamma^3, \gamma^2, \gamma^4\}, \{\gamma^3, \gamma^6, \gamma^5\}\},$$

where each block  $B \in W_3$  is with cardinality  $|B| = 3$  and block sum  $\sum_{i \in B} i = 1$  in  $\mathbb{F}_{2^3}$ .

Two results are shown below that the collection  $W_2$  forms a partition of  $X$  and each block in  $W_2$  is not a subset of  $W_k$  for  $k \geq 3$ , so  $W_2$  forms a group set for constructing GDD with respect to  $X$ .

**Lemma 3.4.** The blocks set  $W_2$  forms a partition of  $X$  and the number of blocks in  $W_2$  is  $\frac{2^m-2}{2}$ .

*Proof.* For each  $a \in X$ ,  $0, 1 \notin X$  implies  $a \notin \{0, 1\}$ , so  $a + 1 := b \notin \{0, 1\}$  either. Hence,  $b \in X$ . Besides,  $a \neq b$  since  $a + b = 1 \neq 0$ . Therefore,  $\{a, b\} \in W_2$  and  $W_2$  forms a partition of  $X$ . Then, the number of blocks in  $W_2$  is counted by

$$|W_2| = \frac{|X|}{2} = \frac{|\mathbb{F}_{2^m} \setminus \{0, 1\}|}{2} = \frac{2^m - 2}{2}.$$

□

**Lemma 3.5.** *For each  $k \geq 3$ , a block in  $W_2$  is not a subset of any block in  $W_k$ .*

*Proof.* The result immediately follows from Definition 2.1.  $\square$

It should be noticed that Lemmas 3.4 and 3.5 give the conditions in Definition 2.1 (i) and (ii), respectively, for the triple  $(X, W_2, W_k)$ . Next, in order to prove that the triple  $(X, W_2, W_k)$  is a  $\text{GDD}(2^m - 2, 2, k)$  for positive integers  $m \geq k \geq 3$ , it is sufficient to find a balance parameter  $\lambda_k$ .

First of all, a group divisible design with block size  $k = 3$  is presented.

**Theorem 3.6.** *For  $m \geq 3$ , the triple  $(X, W_2, W_3)$  is a  $\text{GDD}(2^m - 2, 2, 3)$  with balance parameter*

$$\lambda_3 = 1.$$

*Proof.* Given two distinct elements  $u, v \in X = \mathbb{F}_{2^m} \setminus \{0, 1\}$  with  $\{u, v\} \notin W_2$ . Let  $\lambda_3(u, v)$  be the number of blocks in  $W_3$  that contains both  $u$  and  $v$ . Then, by Lemmas 3.4 and 3.5, it suffices to prove that  $\lambda_3(u, v) = 1$ , which is independent of the choice of  $u$  and  $v$ . By letting  $k = 3$  in Definition 3.1, one can see that the only block in  $W_3$  that contains  $u$  and  $v$  is  $\{u, v, u + v + 1\}$ . Note that  $u + v + 1 \in \mathbb{F}_{2^m} \setminus \{0, 1, u, v\}$  since  $u, v$  are two distinct elements in  $X$  with  $\{u, v\} \notin W_2$ . The result follows.  $\square$

Substituting  $v = 2^m - 2$ ,  $n = 2$ , and  $k = 3$  into (2.1) in Proposition 2.2 and (2.2) in Proposition 2.3 gives

$$r_3 = \lambda_3 \cdot \frac{(2^m - 2) - 2}{3 - 1} = \lambda_3 \cdot \frac{2^m - 4}{2}$$

and

$$b_3 = r_3 \cdot \frac{2^m - 2}{3},$$

respectively. Therefore Corollary 3.7 follows.

**Corollary 3.7.** *The repetition number of the triple  $(X, W_2, W_3)$  is*

$$r_3 = \frac{2^m - 4}{2!}$$

*and the number of blocks in  $W_3$  is*

$$|W_3| = b_3 = \frac{(2^m - 2)(2^m - 4)}{3!}.$$

$\square$

Several blocks sets, which will be used in the proofs of the theorems, are defined.

**Definition 3.8.** Given two distinct elements  $u, v \in X$  with  $\{u, v\} \notin W_2$ . Let  $z = u + v$  and  $S = \{u, v, u + 1, v + 1\}$ . For each  $k \geq 3$ , define the blocks sets

$$\begin{aligned}\Omega_{z,k} &= \{B \in W_k \mid z \in B\}, \\ \omega_{\alpha,k} &= \{B \in \Omega_{z,k} \mid \alpha \in B \setminus \{z\}\} \quad \text{for each } \alpha \in S, \quad \text{and} \\ \tau_{\alpha,k} &= \{B \in \Omega_{z,k} \mid \exists a, b \in B \setminus \{z\} \text{ such that } a + b = \alpha\} \quad \text{for each } \alpha \in S.\end{aligned}$$

Below, Example 3.3 is reviewed in order to realize the blocks sets defined in Definition 3.8.

**Example 3.9.** As stated in Example 3.3,  $X = \{\gamma^i \mid i = 1, 2, \dots, 6\}$ , where the elements are defined as  $\gamma = x$ ,  $\gamma^2 = x^2$ ,  $\gamma^3 = x + 1$ ,  $\gamma^4 = x^2 + x$ ,  $\gamma^5 = x^2 + x + 1$ , and  $\gamma^6 = x^2 + 1$ . The collection  $W_3$  of 3-subsets of  $X$  is

$$W_3 = \{\{\gamma, \gamma^2, \gamma^5\}, \{\gamma, \gamma^6, \gamma^4\}, \{\gamma^3, \gamma^2, \gamma^4\}, \{\gamma^3, \gamma^6, \gamma^5\}\}.$$

Let  $u = \gamma$  and  $v = \gamma^2$ . Thus,  $u + 1 = \gamma^3$ ,  $v + 1 = \gamma^6$ , and  $z = u + v = x + x^2 = \gamma^4$ . Finally, five blocks subsets of  $W_3$  are

$$\begin{aligned}\Omega_{z,3} &= \{\{\gamma, \gamma^6, \gamma^4\}, \{\gamma^3, \gamma^2, \gamma^4\}, \{\gamma^3, \gamma^6, \gamma^5\}\} \\ \omega_{u,3} &= \omega_{v+1,3} = \{\{\gamma, \gamma^6, \gamma^4\}\}, \quad \text{and} \\ \omega_{v,3} &= \omega_{u+1,3} = \{\{\gamma^3, \gamma^2, \gamma^4\}\}.\end{aligned}$$

Example 3.9 illustrates the case for  $m = k = 3$ , and it is easy to see that  $\tau_{\alpha,3} = \emptyset$  for  $\alpha \in S$ . An example for the case  $m = k = 4$  is further presented.

**Example 3.10.** Let  $m = 4$ . Let  $\gamma = x$  be a primitive element of the finite field  $\mathbb{F}_{2^4} \cong \mathbb{F}_2[x]/\langle x^4 + x + 1 \rangle$ . Then,  $X = \{\gamma^i \mid i = 1, 2, \dots, 14\}$ , where the elements are presented as follows:

$i$	$\gamma^i$	$8$	$x^2 + 1$
$2$	$x^2$	$9$	$x^3 + x$
$3$	$x^3$	$10$	$x^2 + x + 1$
$4$	$x + 1$	$11$	$x^3 + x^2 + x$
$5$	$x^2 + x$	$12$	$x^3 + x^2 + x + 1$
$6$	$x^3 + x^2$	$13$	$x^3 + x^2 + 1$
$7$	$x^3 + x + 1$	$14$	$x^3 + 1$

Let  $u = \gamma$  and  $v = \gamma^2$ . It is not difficult to check that  $u + 1 = \gamma^4$ ,  $v + 1 = \gamma^8$ , and  $z = u + v = x + x^2 = \gamma^5$ . For  $\alpha, \beta \in S = \{u, v, u + 1, v + 1\}$ , the blocks subsets  $\Omega_{z,4}$ ,  $\omega_{\alpha,4}$ , and  $\tau_{\beta,4}$  of  $W_4$  can be written as

$$\begin{aligned}
\Omega_{z,4} &= \left\{ \begin{array}{lll} \{\gamma^5, \gamma, \gamma^3, \gamma^{13}\}, & \{\gamma^5, \gamma, \gamma^6, \gamma^{14}\}, & \{\gamma^5, \gamma, \gamma^7, \gamma^{11}\}, \\ \{\gamma^5, \gamma, \gamma^9, \gamma^{12}\}, & \{\gamma^5, \gamma^2, \gamma^3, \gamma^7\}, & \{\gamma^5, \gamma^2, \gamma^6, \gamma^{12}\}, \\ \{\gamma^5, \gamma^2, \gamma^9, \gamma^{14}\}, & \{\gamma^5, \gamma^2, \gamma^{11}, \gamma^{13}\}, & \{\gamma^5, \gamma^3, \gamma^4, \gamma^6\}, \\ \{\gamma^5, \gamma^3, \gamma^8, \gamma^9\}, & \{\gamma^5, \gamma^4, \gamma^7, \gamma^{12}\}, & \{\gamma^5, \gamma^4, \gamma^9, \gamma^{11}\}, \\ \{\gamma^5, \gamma^4, \gamma^{13}, \gamma^{14}\}, & \{\gamma^5, \gamma^6, \gamma^8, \gamma^{11}\}, & \{\gamma^5, \gamma^7, \gamma^8, \gamma^{14}\}, \\ \{\gamma^5, \gamma^8, \gamma^{12}, \gamma^{13}\} \end{array} \right\}, \\
\omega_{u,4} &= \tau_{v+1,4} \\
&= \{\{\gamma^5, \gamma, \gamma^3, \gamma^{13}\}, \{\gamma^5, \gamma, \gamma^6, \gamma^{14}\}, \{\gamma^5, \gamma, \gamma^7, \gamma^{11}\}, \{\gamma^5, \gamma, \gamma^9, \gamma^{12}\}\}, \\
\omega_{v,4} &= \tau_{u+1,4} \\
&= \{\{\gamma^5, \gamma^2, \gamma^3, \gamma^7\}, \{\gamma^5, \gamma^2, \gamma^6, \gamma^{12}\}, \{\gamma^5, \gamma^2, \gamma^9, \gamma^{14}\}, \{\gamma^5, \gamma^2, \gamma^{11}, \gamma^{13}\}\}, \\
\omega_{u+1,4} &= \tau_{v,4} \\
&= \{\{\gamma^5, \gamma^4, \gamma^7, \gamma^{12}\}, \{\gamma^5, \gamma^3, \gamma^4, \gamma^6\}, \{\gamma^5, \gamma^4, \gamma^7, \gamma^{12}\}, \{\gamma^5, \gamma^4, \gamma^{13}, \gamma^{14}\}\}, \\
&\text{and} \\
\omega_{v+1,4} &= \tau_{u,4} \\
&= \{\{\gamma^5, \gamma^3, \gamma^8, \gamma^9\}, \{\gamma^5, \gamma^6, \gamma^8, \gamma^{11}\}, \{\gamma^5, \gamma^7, \gamma^8, \gamma^{14}\}, \{\gamma^5, \gamma^8, \gamma^{12}, \gamma^{13}\}\}.
\end{aligned}$$

The detailed results of the blocks subsets of  $W_k$  are provided in the following lemma.

**Lemma 3.11.** *The relations between the blocks sets in Definition 3.8 are described below.*

- (i)  $\omega_{\alpha,k}, \tau_{\beta,k} \subset \Omega_{z,k}$  for  $\alpha, \beta \in S$ .
- (ii)  $\omega_{u,3} = \omega_{v+1,3}$  and  $\omega_{v,3} = \omega_{u+1,3}$ . If  $k \geq 4$ , then  $\omega_{\alpha,k} \cap \omega_{\beta,k} = \phi$  for distinct  $\alpha, \beta \in S$ .
- (iii)  $\omega_{u,4} = \tau_{v+1,4}$  and  $\omega_{v,4} = \tau_{u+1,4}$ . If  $k \geq 5$ , then  $\omega_{\alpha,k} \cap \tau_{\beta,k} = \phi$  for  $\alpha, \beta \in S$ .
- (iv)  $\tau_{u,5} = \tau_{v+1,5}$  and  $\tau_{v,5} = \tau_{u+1,5}$ . If  $k \geq 6$ , then  $\tau_{\alpha,k} \cap \tau_{\beta,k} = \phi$  for distinct  $\alpha, \beta \in S$ .



*Proof.* (i) is directly from Definition 3.8.

To prove (ii), it follows from Definition 3.8 that  $\omega_{\alpha,3} = \omega_{\alpha+u+v+1,3}$  since  $z + u + v + 1 = 1$ . For  $k \geq 4$ , suppose to the contrary that there exists  $B \in \omega_{\alpha,k} \cap \omega_{\beta,k}$  for some distinct  $\alpha, \beta \in S$ . Then,  $\alpha, \beta, z \in B$ . Note that  $\alpha + \beta \in \{1, u + v, u + v + 1\}$ . If  $\alpha + \beta = 1$ , then it contradicts to the definition that  $\binom{B}{2} \cap W_2 = \phi$ . If  $\alpha + \beta \in \{u + v, u + v + 1\}$ , then  $\alpha + \beta + z \in \{0, 1\}$  which also contradicts to Remark 3.2.

To verify (iii), Definition 3.8 indicates that  $\omega_{\alpha,4} = \tau_{\alpha+u+v+1,4}$  since  $z + u + v + 1 = 1$ . For  $k \geq 5$ , suppose to the contrary that there exists  $B \in \omega_{\alpha,k} \cap \tau_{\beta,k}$  for some  $\alpha, \beta \in S$ . Let distinct  $a, b \in B$  such that  $a + b = \beta$ . Assume that  $a, b$  are both not  $\alpha$ . Then,  $\alpha + a + b \in \{0, 1, u + v, u + v + 1\}$ . If  $\alpha + a + b \in \{0, 1\}$  then it contradicts to Remark 3.2. If  $\alpha + a + b \in \{u + v, u + v + 1\}$ , then  $z + \alpha + a + b \in \{0, 1\}$ , which also contradicts to Remark 3.2. Thus, without loss of generality, suppose  $a = \alpha$ . Then,  $b = \alpha + \beta$ . Since  $b \notin \{0, 1\}$ ,  $b \in \{u + v, u + v + 1\}$ . However, it is easily seen that  $b + z \in \{0, 1\}$ , which contradicts to Remark 3.2.

To prove (iv), it is directly from Definition 3.8 that  $\tau_{\alpha,5} = \tau_{\alpha+u+v+1,5}$  since  $z + u + v + 1 = 1$ . For  $k \geq 6$ , suppose to the contrary that there exists  $B \in \tau_{\alpha,k} \cap \tau_{\beta,k}$  for some distinct  $\alpha, \beta \in S$ . Let distinct  $a, b \in B$  and distinct  $c, d \in B$  such that  $a + b = \alpha$  and  $c + d = \beta$ . Assume that  $\{a, b\} \cap \{c, d\} = \phi$ . Then,  $a + b + c + d \in \{0, 1, u + v, u + v + 1\}$ . If  $a + b + c + d \in \{0, 1\}$  then it contradicts to Remark 3.2. If  $a + b + c + d \in \{u + v, u + v + 1\}$ , then  $z + a + b + c + d \in \{0, 1\}$ , which also contradicts to Remark 3.2. Thus, without loss of generality, suppose  $a = c$ . Then,  $b + d = \alpha + \beta \in \{0, 1, u + v, u + v + 1\}$ . If  $b + d \in \{0, 1\}$ , then it contradicts to Remark 3.2. If  $b + d \in \{u + v, u + v + 1\}$ , then  $z + b + d \in \{0, 1\}$ , which also contradicts to Remark 3.2. The proof of this lemma is complete.  $\square$

**Lemma 3.12.** *Given two distinct elements  $u, v \in X$  and  $z = u + v$ . Then*

for each  $\alpha \in S = \{u, v, u+1, v+1\}$ ,

$$\begin{aligned}
|\Omega_{z,k}| &= r_k \quad \text{for } k \geq 4, \\
|\omega_{\alpha,k}| &= \lambda_k \quad \text{for } k \geq 4, \\
|\tau_{\alpha,4}| &= \frac{1}{2}(2^m - 2^3) \quad \text{for } m \geq 4, \\
|\tau_{\alpha,5}| &= \frac{1}{4}(2^m - 2^3)(2^m - 2^4) \quad \text{for } m \geq 5, \quad \text{and} \\
|\tau_{\alpha,6}| &= \frac{1}{12}(2^m - 2^3)(2^m - 2^4)(2^m - 2^5) \quad \text{for } m \geq 6.
\end{aligned}$$

*Proof.* Note that  $|\omega_{\alpha,k}| = |\omega_{\beta,k}|$  and  $|\tau_{\alpha,k}| = |\tau_{\beta,k}|$  for any  $\alpha, \beta \in S$  because of the symmetry. Fixed some  $\alpha \in S$ , the cardinalities of  $\Omega_{z,k}$  and  $\omega_{\alpha,k}$  are from the definition of the repetition number  $r_k$  and balance parameter  $\lambda_k$ , respectively.

To count  $|\tau_{\alpha,4}|$ , let  $B \in \tau_{\alpha,4}$  such that  $B = \{z, a, \alpha+a, z+\alpha+1\}$  without loss of generality. Note that  $B \subset X = \mathbb{F}_{2^m} \setminus \{0, 1\}$  and by Remark 3.2,  $\binom{B}{2} \cap W_2 = \binom{B}{3} \cap W_3 = \phi$ . Hence  $a$  can be chosen from

$$\mathbb{F}_{2^m} \setminus (\{0, 1\} + \{0, u\} + \{0, v\}) = \mathbb{F}_{2^m} \setminus \{0, 1, u, u+1, v, v+1, u+v, u+v+1\}$$

where the addition  $+$  between two subsets  $A, B$  of  $\mathbb{F}_{2^m}$  is defined as  $A+B = \{i+j \mid i \in A \text{ and } j \in B\}$ . Since the two elements  $a$  and  $\alpha+a$  are not ordered, there are  $\frac{2^m-2^3}{2}$  ways to determine  $B$ , which implies  $|\tau_{\alpha,4}| = \frac{1}{2}(2^m - 2^3)$ .

To count  $|\tau_{\alpha,5}|$ , let  $B \in \tau_{\alpha,5}$  such that  $B = \{z, a, \alpha+a, b, z+\alpha+1+b\}$  without loss of generality. There are  $\frac{2^m-2^3}{2}$  ways to determine the elements  $a$  and  $\alpha+a$  from the argument of counting  $|\tau_{\alpha,4}|$ . Note that  $B \subset X$  and by Remark 3.2 we have  $\binom{B}{2} \cap W_2 = \binom{B}{3} \cap W_3 = \binom{B}{4} \cap W_4 = \phi$ . Hence,  $b$  can be chosen from

$$\mathbb{F}_{2^m} \setminus (\{0, 1\} + \{0, u\} + \{0, v\} + \{0, a\}).$$

Since the two elements  $b$  and  $z+\alpha+1+b$  are not ordered, there are  $\frac{2^m-2^4}{2}$  ways to determine them, which implies

$$|\tau_{\alpha,5}| = \frac{1}{2}(2^m - 2^3) \cdot \frac{1}{2}(2^m - 2^4) = \frac{1}{4}(2^m - 2^3)(2^m - 2^4).$$

To count  $|\tau_{\alpha,6}|$ , let  $B \in \tau_{\alpha,6}$  such that  $B = \{z, a, \alpha+a, b, c, z+\alpha+1+b+c\}$  without loss of generality. There are  $\frac{2^m-2^3}{2}$  ways to determine the elements  $a$

and  $\alpha + a$  from the argument of counting  $|\tau_{\alpha,4}|$ . Similar with the lower part of counting  $|\tau_{\alpha,5}|$ , there are  $(2^m - 2^4)$  ways to pick  $b$ , and then  $(2^m - 2^5)$  ways to pick  $c$ . Since the three elements  $b$ ,  $c$  and  $z + \alpha + 1 + b + c$  are not ordered, there are  $\frac{1}{3!}(2^m - 2^4)(2^m - 2^5)$  ways to determine them, which implies

$$|\tau_{\alpha,6}| = \frac{1}{2}(2^m - 2^3) \cdot \frac{1}{3!}(2^m - 2^4)(2^m - 2^5) = \frac{1}{12}(2^m - 2^3)(2^m - 2^4)(2^m - 2^5).$$

□

The blocks sets introduced in Definition 3.8 will be used to construct group divisible designs with block size 4, 5, 6 and 7.

We are now ready to present a GDD with block size 4. The cardinalities  $|\Omega_{z,3}|$  and  $|\omega_{\alpha,3}|$  found in Lemma 3.12 help in counting the parameter  $\lambda_4$ .

**Theorem 3.13.** *If  $m \geq 4$ , then the triple  $(X, W_2, W_4)$  is a  $GDD(2^m - 2, 2, 4)$  with balance parameter*

$$\lambda_4 = \frac{2^m - 8}{2}.$$

*Proof.* Given two distinct elements  $u, v \in X$  with  $\{u, v\} \notin W_2$ . Let  $\lambda_4(u, v)$  be the number of blocks in  $W_4$  that contains both  $u$  and  $v$ . Let  $z = u + v$  and  $S = \{u, v, u + 1, v + 1\}$ . The blocks sets  $\Omega_{z,3}$  and  $\omega_{\alpha,3}$  for  $\alpha \in S$  are mentioned in Definition 3.8.

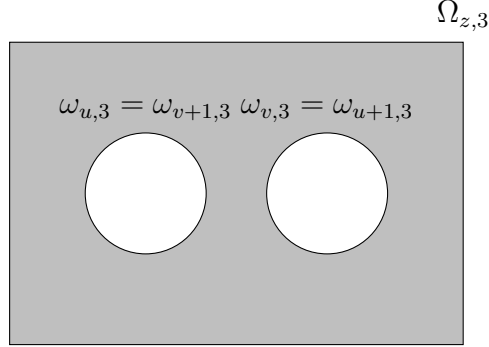
Note that a block  $B \in W_4$  that contains both  $u$  and  $v$  corresponds to a unique block  $\overline{B} \in \Omega_{z,3}$  such that  $B \setminus \{u, v\} = \overline{B} \setminus \{z\}$ . However, according to the above corresponding rule, for each block  $B \in W_4$ ,  $|B| = 4$  and  $\binom{B}{2} \cap W_2 = \emptyset$  imply  $S \cap \overline{B} = \emptyset$ . Applying Lemma 3.11 (ii) and the cardinalities  $|\Omega_{z,3}|$ ,  $|\omega_{u,3}|$  given in Lemma 3.12 yields

$$\lambda_4(u, v) = |\Omega_{z,3}| - 2|\omega_{u,3}| = r_3 - 2\lambda_3.$$

The Venn diagram for  $\Omega_{z,3}$  is shown in Figure 1. Moreover, from the values of  $\lambda_3$  in Theorem 3.6 and  $r_3$  in Corollary 3.7, one has

$$\lambda_4(u, v) = \frac{2^m - 4}{2!} - 2 = \frac{2^m - 8}{2!},$$

which is independent of the choice of  $x$  and  $y$ . The desired conclusion follows. □



**Figure 1:** The Venn diagram for the proof of Theorem 3.13.

Substituting  $v = 2^m - 2$ ,  $n = 2$ , and  $k = 3$  into (2.1) in Proposition 2.2 and (2.2) in Proposition 2.3 gives

$$r_4 = \lambda_4 \cdot \frac{(2^m - 2) - 2}{4 - 1} = \lambda_4 \cdot \frac{2^m - 4}{3}$$

and

$$b_4 = r_4 \cdot \frac{2^m - 2}{4},$$

respectively. Thus one has Corollary 3.14.

**Corollary 3.14.** *The repetition number of the triple  $(X, W_2, W_4)$  is*

$$r_4 = \frac{(2^m - 4)(2^m - 8)}{3!}$$

*and the number of blocks in  $W_4$  is*

$$|W_4| = b_4 = \frac{(2^m - 2)(2^m - 4)(2^m - 8)}{4!}.$$

□

A group divisible design with block size 5 is proposed. To count the parameter  $\lambda_5$ , the cardinalities  $|\Omega_{z,4}|$ ,  $|\omega_{\alpha,4}|$ , and  $|\tau_{\beta,4}|$  obtained in Lemma 3.12 are used.

**Theorem 3.15.** *If  $m \geq 5$ , then the triple  $(X, W_2, W_5)$  is a GDD $(2^m - 2, 2, 5)$  with balance parameter*

$$\lambda_5 = \frac{(2^m - 8)(2^m - 16)}{3!}.$$

*Proof.* First, consider two distinct elements  $u, v \in X$  with  $\{u, v\} \notin W_2$ . Let  $\lambda_5(x, y)$  be the number of blocks in  $W_5$  that contains both  $u$  and  $v$ . Owing to  $z = u + v$  and  $S = \{u, v, u + 1, v + 1\}$ , the blocks sets  $\Omega_{z,4}$ ,  $\omega_{\alpha,4}$ , and  $\tau_{\alpha,4}$  for  $\alpha \in S$  are known from Definition 3.8.

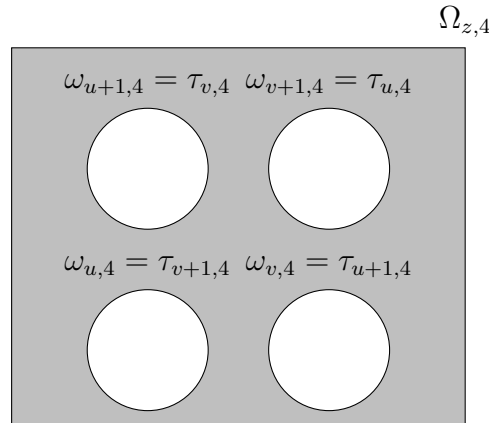
It is important to note that a block  $B \in W_5$  that contain both  $u$  and  $v$  corresponds to a unique block  $\overline{B} \in \Omega_{z,4}$  such that  $B \setminus \{u, v\} = \overline{B} \setminus \{z\}$ . However, for each block  $B \in W_5$ ,  $|B| = 5$  implies  $u, v \notin \overline{B}$ , and  $\binom{B}{2} \cap W_2 = \emptyset$  implies  $u + 1, v + 1 \notin \overline{B}$ . As a consequence of Lemma 3.11 (iii) and the cardinalities  $|\Omega_{z,4}|$ ,  $|\omega_{u,4}|$  obtained in Lemma 3.12, we have

$$\lambda_5(u, v) = |\Omega_{z,4}| - 4|\omega_{u,4}| = r_4 - 4\lambda_4,$$

where the Venn diagram for  $\Omega_{z,4}$  is depicted in Figure 2. In accordance with the values of  $\lambda_4$  in Theorem 3.13 and  $r_4$  in Corollary 3.14, the parameter  $\lambda_5$  can be further expressed as

$$\lambda_5(u, v) = \frac{(2^m - 4)(2^m - 8)}{3!} - 4\frac{2^m - 8}{2!} = \frac{(2^m - 8)(2^m - 16)}{3!},$$

which is independent of the choice of  $u$  and  $v$ . The proof of this theorem is completed.  $\square$



**Figure 2:** The Venn diagram for the proof of Theorem 3.15.

Substituting  $v = 2^m - 2$ ,  $n = 2$ , and  $k = 5$  into (2.1) in Proposition 2.2 and (2.2) in Proposition 2.3 leads to

$$r_5 = \lambda_5 \cdot \frac{(2^m - 2) - 2}{5 - 1} = \lambda_3 \cdot \frac{2^m - 4}{4}$$

and

$$b_5 = r_5 \cdot \frac{2^m - 2}{5},$$

respectively. Hence Corollary 3.16 follows.

**Corollary 3.16.** *The repetition number of the triple  $(X, W_2, W_5)$  is*

$$r_5 = \frac{(2^m - 4)(2^m - 8)(2^m - 16)}{4!}$$

*and the number of blocks in  $W_5$  is*

$$|W_5| = b_5 = \frac{(2^m - 2)(2^m - 4)(2^m - 8)(2^m - 16)}{5!}.$$

□

A group divisible design with block size 6 is presented. The cardinalities  $|\Omega_{z,5}|$ ,  $|\omega_{\alpha,5}|$ , and  $|\tau_{\beta,5}|$  found in Lemma 3.12 are applied to calculate the parameter  $\lambda_6$ .

**Theorem 3.17.** *If  $m \geq 6$ , then the triple  $(X, W_2, W_6)$  is a  $GDD(2^m - 2, 2, 6)$  with balance parameter*

$$\lambda_6 = \frac{(2^m - 8)(2^m - 16)(2^m - 32)}{4!}.$$

*Proof.* Given two distinct elements  $u, v \in X$  with  $\{u, v\} \notin W_2$ , denote the number of blocks in  $W_6$  that contains both  $u$  and  $v$  by  $\lambda_6(u, v)$ . If  $z = x + y$  and  $S = \{u, v, u + 1, v + 1\}$ , then the blocks sets  $\Omega_{z,5}$ ,  $\omega_{\alpha,5}$ , and  $\tau_{\alpha,5}$  for  $\alpha \in S$  can be derived from Definition 3.8. A block  $B \in W_6$  that contains both  $x$  and  $y$  corresponds to a unique block  $\overline{B} \in \Omega_{z,5}$  such that  $B \setminus \{u, v\} = \overline{B} \setminus \{z\}$ . For each block  $B \in W_6$ , we have

- (i)  $|B| = 6$  implies  $x, y \notin \overline{B}$ ,
- (ii)  $\binom{B}{2} \cap W_2 = \emptyset$  implies  $u + 1, v + 1 \notin \overline{B}$ , and

(iii)  $\binom{B}{3} \cap W_3 = \phi$  implies  $\nexists a, b \in \overline{B} \setminus \{z\}$  such that  $a+b \in \{u, v, u+1, v+1\}$ .

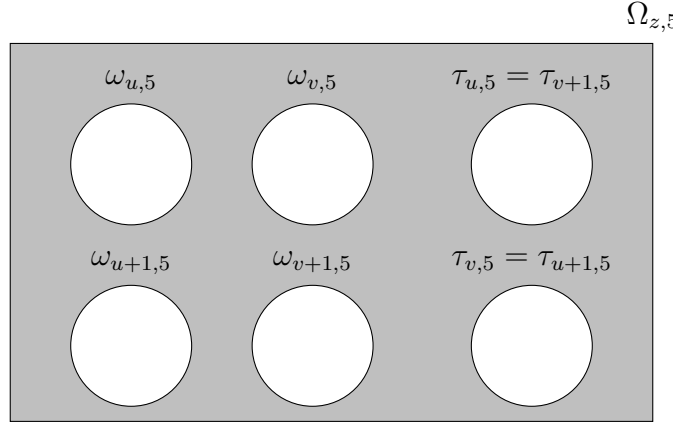
Note that the third condition  $\binom{B}{3} \cap W_3 = \phi$  is equivalent to that there do not exist three distinct elements in  $B$  with sum in  $\{0, 1\}$ . Thus, by Lemma 3.11 (iii) and the cardinalities  $|\Omega_{z,5}|$ ,  $|\omega_{u,5}|$ , and  $|\tau_{u,5}|$  given in Lemma 3.12, we have

$$\lambda_6(u, v) = |\Omega_{z,5}| - 4|\omega_{u,5}| - 2|\tau_{u,5}| = r_5 - 4\lambda_5 - \frac{1}{2}(2^m - 8)(2^m - 16).$$

The Venn diagram can be seen in Figure 3. Furthermore, from the values of  $\lambda_5$  and  $r_5$  respectively given in Theorem 3.15 and Corollary 3.16,

$$\lambda_6(u, v) = \frac{(2^m - 8)(2^m - 16)(2^m - 32)}{4!},$$

which is independent of the choice of  $u$  and  $v$ . The desired result is obtained.  $\square$



**Figure 3:** The Venn diagram for the proof of Theorem 3.17.

Substituting  $v = 2^m - 2$ ,  $n = 2$ , and  $k = 6$  into (2.1) in Proposition 2.2 and (2.2) in Proposition 2.3 yields

$$r_6 = \lambda_6 \cdot \frac{(2^m - 2) - 2}{6 - 1} = \lambda_6 \cdot \frac{2^m - 4}{5}$$

and

$$b_6 = r_6 \cdot \frac{2^m - 2}{6},$$

respectively. Hence one has Corollary 3.18.

**Corollary 3.18.** *The repetition number of the triple  $(X, W_2, W_6)$  is*

$$r_6 = \frac{(2^m - 4)(2^m - 8)(2^m - 16)(2^m - 32)}{5!}$$

*and the number of blocks in  $W_6$  is*

$$|W_6| = b_6 = \frac{(2^m - 2)(2^m - 4)(2^m - 8)(2^m - 16)(2^m - 32)}{6!}.$$

□

The next theorem states a group divisible design with block size 7. The cardinalities  $|\Omega_{z,6}|$ ,  $|\omega_{\alpha,6}|$ , and  $|\tau_{\beta,6}|$  found in Lemma 3.12 play an important role in determining the parameter  $\lambda_7$ .

**Theorem 3.19.** *If  $m \geq 7$ , then the triple  $(X, W_2, W_7)$  is a  $GDD(2^m - 2, 2, 7)$  with balance parameter*

$$\lambda_7 = \frac{(2^m - 8)(2^m - 16)(2^m - 32)(2^m - 64)}{5!}.$$

*Proof.* Given two distinct elements  $u, v \in X$  with  $\{u, v\} \notin W_2$ , let  $\lambda_7(u, v)$  be the number of blocks in  $W_7$  that contains both  $u$  and  $v$ . Let  $z = u + v$  and  $S = \{u, v, u + 1, v + 1\}$ . A block  $B \in W_7$  that contains both  $x$  and  $y$  corresponds to a unique block  $\overline{B} \in \Omega_{z,6}$  such that  $B \setminus \{u, v\} = \overline{B} \setminus \{z\}$ , where the blocks set  $\Omega_{z,6}$  is defined in Definition 3.8 and depicted in Figure 4. For each block  $B \in W_6$ , we have

- (i)  $|B| = 6$  implies  $u, v \notin \overline{B}$ ,
- (ii)  $\binom{B}{2} \cap W_2 = \emptyset$  implies  $u + 1, v + 1 \notin \overline{B}$ ,
- (iii)  $\binom{B}{3} \cap W_3 = \emptyset$  implies  $\nexists a, b \in \overline{B} \setminus \{z\}$  such that  $a + b \in \{u + 1, v + 1\}$ ,  
and
- (iv)  $\binom{B}{4} \cap W_4 = \emptyset$  implies  $\nexists a, b \in \overline{B} \setminus \{z\}$  such that  $a + b \in \{u, v\}$ .

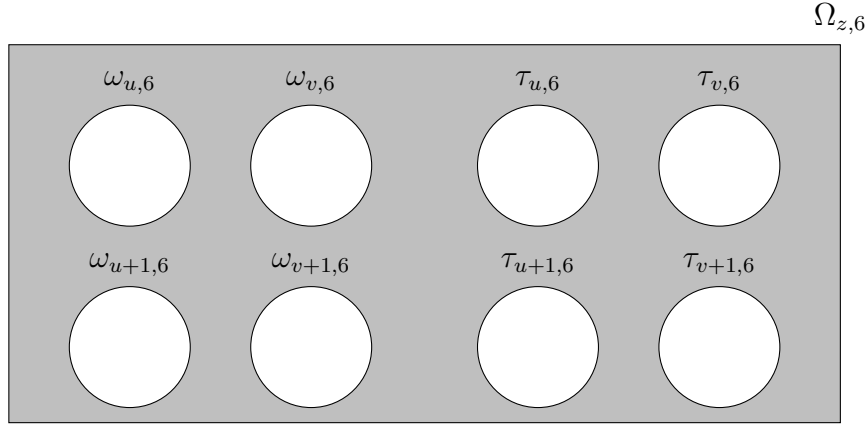
Using  $\omega_{\alpha,6}$  and  $\tau_{\alpha,6}$  for  $\alpha \in S = \{u, v, u + 1, v + 1\}$  in Definition 3.8 and combining all results in Lemma 3.11 (iv), the cardinalities  $|\Omega_{z,6}|$ ,  $|\omega_{u,6}|$  and



$|\tau_{u,6}|$  in Lemma 3.12, the value of  $\lambda_6$  in Theorem 3.17, and the amount of  $r_6$  in Corollary 3.18, the parameter  $\lambda_7$  finally becomes

$$\begin{aligned}\lambda_7(u, v) &= |\Omega_{z,6}| - 4|\omega_{u,6}| - 4|\tau_{u,6}| \\ &= r_6 - 4\lambda_6 - \frac{1}{3}(2^m - 8)(2^m - 16)(2^m - 32) \\ &= \frac{(2^m - 8)(2^m - 16)(2^m - 32)(2^m - 64)}{5!},\end{aligned}$$

which is independent of the choice of  $u$  and  $v$ . This completes the proof.  $\square$



**Figure 4:** The Venn diagram for the proof of Theorem 3.19.

Corollary 3.20 is easily carried out according to the formulas  $r = \lambda(v - n)/(k - 1)$  in Proposition 2.2 and  $b = vr/k$  in Proposition 2.3.

**Corollary 3.20.** *The repetition number of the triple  $(X, W_2, W_7)$  is*

$$r_7 = \frac{(2^m - 4)(2^m - 8)(2^m - 16)(2^m - 32)(2^m - 64)}{6!}$$

*and the number of blocks in  $W_7$  is*

$$|W_7| = b_7 = \frac{(2^m - 2)(2^m - 4)(2^m - 8)(2^m - 16)(2^m - 32)(2^m - 64)}{7!}.$$

$\square$

## 4 Concluding remark

This paper has demonstrated that the triple  $(X, W_2, W_k)$  is a GDD $(2^m - 2, 2, k)$  for  $k = 3, 4, 5, 6, 7$  and  $m \geq k$ . The balance parameter  $\lambda_k$ , repetition number  $r_k$  and number of blocks  $b_k$  of each GDD are shown in Table 1.

**Table 1:** The balance parameter  $\lambda_k$ , repetition number  $r_k$  and number of blocks  $b_k$  of triple  $(X, W_2, W_k)$  for  $k = 3, 4, 5, 6$ , and  $7$ , respectively.

	$\lambda_k$	$r_k$	$b_k$
$k = 3$	1	$\frac{2^m-4}{2!}$	$\frac{(2^m-2)(2^m-4)}{3!}$
$k = 4$	$\frac{2^m-8}{2!}$	$\frac{(2^m-4)(2^m-8)}{3!}$	$\frac{(2^m-2)(2^m-4)(2^m-8)}{4!}$
$k = 5$	$\frac{(2^m-8)(2^m-16)}{3!}$	$\frac{(2^m-4)(2^m-8)(2^m-16)}{4!}$	$\frac{(2^m-2)(2^m-4)(2^m-8)(2^m-16)}{5!}$
$k = 6$	$\frac{\prod_{i=3}^5 (2^m-2^i)}{4!}$	$\frac{\prod_{i=2}^5 (2^m-2^i)}{5!}$	$\frac{\prod_{i=1}^5 (2^m-2^i)}{6!}$
$k = 7$	$\frac{\prod_{i=3}^6 (2^m-2^i)}{5!}$	$\frac{\prod_{i=2}^6 (2^m-2^i)}{6!}$	$\frac{\prod_{i=1}^6 (2^m-2^i)}{7!}$

By observing the above table, we give a conjecture that the triple  $(X, W_2, W_k)$  is a GDD for all  $m \geq k \geq 3$  including the exact values for the parameters  $\lambda_k$ ,  $r_k$ , and  $b_k$ .

**Conjecture 4.1.** For  $m \geq k \geq 3$ , let

$$W_k = \left\{ \left\{ x_1, x_2, \dots, x_k \right\} \subset X \left| \begin{array}{l} \sum_{i=1}^k x_i = 1, \text{ and } \sum_{i \in I} x_i \neq 1 \text{ for each} \\ \text{nonempty proper subset } I \subset \{1, 2, \dots, k\} \end{array} \right. \right\}.$$

Then, the triple  $(X, W_2, W_k)$  is a  $GDD(2^m - 2, 2, k)$  with

$$\begin{aligned} \text{balance parameter} \quad \lambda_k &= \frac{\prod_{i=3}^{k-1} (2^m - 2^i)}{(k-2)!}, \\ \text{repetition number} \quad r_k &= \frac{\prod_{i=2}^{k-1} (2^m - 2^i)}{(k-1)!}, \quad \text{and} \\ \text{number of blocks} \quad b_k &= \frac{\prod_{i=1}^{k-1} (2^m - 2^i)}{k!}. \end{aligned}$$

The cases  $k \leq 7$  of Conjecture 4.1 has been proved in this paper by using the including-excluding principle. Due to the complication for larger  $k$ , the key behind the proof might contain other counting methods.

## Acknowledgments

This research is supported by the Ministry of Science and Technology of Taiwan R.O.C. under the project MOST 103-2632-M-214-001-MY3-2 including its subproject MOST 104-2811-M-214-001.

## References

- [1] I. Anderon, *Combinatorial Designs: Construction Methods*, Ellis Horwood, 1990.
- [2] E.F. Assmus, Jr., H.F. Mattson, Jr., New 5-designs, *J. Combin. Theory* 6 (1969) 122-151.
- [3] E.F. Assmus, Jr., H.F. Mattson, Jr., Coding and combinatorics, *SIAM Rev.* 16 (1974) 349-388.
- [4] M. Braun, A. Kohnert, P.R.J. Östergård, A. Wassermann, Large sets of  $t$ -designs over finite fields, *J. Combin. Theory Ser. A* 124 (2014) 195-202.
- [5] C. Bachoc, P. Gaborit, Designs and self-dual codes with long shadows, *J. Combin. Theory Ser. A* 5 (2004) 15-34.

- [6] C.J. Colbourn, J.H. Dinitz, *Handbook of combinatorial designs*, Taylor & Francis Group LLC 2007.
- [7] Y.M. Chee, G. Ge, A.C.H. Ling, Group divisible codes and their application in the construction of optimal constant-composition codes of weight three, *IEEE Trans. Inf. Theory* 54 (2008) 3552-3564.
- [8] Y.M. Chee, S. Ling, Constructions of  $q$ -ary constant-weight codes, *IEEE Trans. Inf. Theory* 53 (2007) 135-146.
- [9] Y.M. Chee, A.C.H. Ling, S. Ling, H. Shen, The PBD-closure of constant-composition codes, *IEEE Trans. Inf. Theory* 53 (2007) 2685-2692.
- [10] Y. Chang, T.K. Truong, I.S. Reed, H.Y. Cheng, C.D. Lee, Algebraic decoding of  $(71, 36, 11)$ ,  $(79, 40, 15)$ , and  $(97, 49, 15)$  quadratic residue codes, *IEEE Trans. on Communications*, 51 (2003) 1463-1473.
- [11] A. Fazeli, S. Lovett, A. Vardy, Nontrivial  $t$ -designs over finite fields exist for all  $t$ , *J. Combin. Theory Ser. A* 127 (2014) 149-160.
- [12] H.L. Fu, C.A. Rodger, Group divisible designs with two associate classes:  $n = 2$  or  $m = 2$ , *J. Combin. Theory Ser. A* 83 (1998) 94-117.
- [13] S.P. Hurd, D.G. Sarvate, Odd and even group divisible designs with two groups and block size four, *Discrete Math.* 284 (2004) 189-196.
- [14] G.T. Kenndy, V. Pless, On designs and formally self-dual codes, *Des. Codes Crypto.* 4 (1994) 43-55.
- [15] V. Pless, Symmetry codes over GF(3) and new five-designs, *J. Combin. Theory Ser. A* 12 (1972) 119-142.
- [16] V. Pless, *Introduction to the Theory of Error-Correction Codes 3rd ed.*, John Wiley & Sons Inc. 1998.
- [17] V. Pless, J.M. Masley, J.S. Leon, On weights in Duadic codes, *J. Combin. Theory Ser. A* 44 (1987) 6-21.
- [18] D.G. Sarvate, J. Seberry, Group divisible designs, GBRSDS, and generalized weighing matrices, *Utilitas Mathematica* 54 (1998) 157-174.

- [19] D.R. Stinson, *Combinatorial designs: constructions and analysis*, Springer-Verlag New York 2004.
- [20] P.J. Tsai, *A construction of group divisible designs*, M.D. Thesis of NUK (Taiwan) 2015.
- [21] Z.X. Wan, *Design Theory*, Higher Education 2009.
- [22] Z.X. Wan, *Finite Field and Galois Rings*, World Scientific 2012.
- [23] L. Wang, Y. Chang, Combinatorial constructions of optimal three-dimensional optical orthogonal codes, *IEEE Trans. Inf. Theory* 61 (2015) 671-687.
- [24] J. Wang, J. Yin, Two-dimensional optimal othorogonal codes and semi-cyclic group divisible designs, *IEEE Trans. Inf. Theory* 56 (2010) 2177-2187.

Chia-an Liu  
 Department of Financial and Computational Mathematics  
 I-Shou University  
 No.1 Sec.1 Xuecheng Rd. Dashu Dist.  
 Kaohsiung, Taiwan 84001 R.O.C.  
 Email: liuchiaan8@gmail.com  
 Ext: +886-7-6577711-5612